§170.315(b)(8) Data segmentation for privacy – receive

2015 Edition Cures Update CCG

Version 1.0 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	06-15-2020

Regulation Text

Regulation Text

§170.315 (b)(8) *Security tags – summary of care – receive.*

(i) Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the:

(A) Document, section, and entry (data element) level; or

(B) Document level for the period until May 2, 2022; and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Standard(s) Referenced

Applies to entire criterion

§ 170.205(a)(4) HL7 Implementation Guide for CDA Release 2 Consolidation CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1 C-CDA 2.1, August 2015, June 2019 (with Errata)

§ 170.205(o)(1) HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

Certification Companion Guide: Security tags - summary of care - receive

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 21st Century Cures Act:

Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Cures Act Final Rule). It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the ONC Cures Act Final Rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Not Included	No

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(b)(8). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(b) "paragraph (b)" criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (b) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "VDT" and (e)(2) "secure messaging," which are explicitly stated.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
  - Amendments (§ 170.315(d)(4))

- Automatic access time-out (§ 170.315(d)(5))
- Emergency access (§ 170.315(d)(6))
- End-user device encryption (§ 170.315(d)(7))
- Integrity (§ 170.315(d)(8))
- Encrypt user credentials (§ 170.315(d)(12))
- Multi-factor authentication (§ 170.315(d)(13))

- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for Approach 1, the health IT developer may certify for the criterion using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces that enable the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- No additional clarifications.

Paragraph (b)(8)(i)

2015 Edition Cures Update Technical outcome - The health IT must be able to receive a summary record (formatted to Consolidated CDA Release 2.1) that is document-level, section, and entry level tagged as restricted and subject to re-disclosure restrictions using the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

Clarifications:

- The DS4P standard does not have a service discovery mechanism to determine if a potential recipient is able to receive a tagged document. We expect that providers will have to determine the receiving capabilities of their exchange partners. This is similar to how providers have to work with their exchange partners today when manually exchanging sensitive health information via fax. [see 80 FR 62648]
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see Frequently Asked Questions #51] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There is a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., Edge Testing Tool: Message Validator - Cures Update C-CDA R2.1 Validator). Similarly, there will be an 18-month delay before a finding of a correction's absence in certified health IT during surveillance would constitute a non-conformity under the Program.

Paragraph (b)(8)(ii)

Technical outcome – The privacy markings must be preserved to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Clarifications:

- No additional clarifications.

Content last reviewed on June 22, 2020